JC20 Rec'd PCT/PTO 14 AUG 2001
Express Mail No. EL652176579US

FORM PTO-1390 (REV 10-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: B-4276PCT 619003-1

U.S. APPLICATION NO. (If known, see 37 CFR 1.5): 09/913453 not yet assigned

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/GB00/00504	15 February 2000	15 February 1999

TITLE OF INVENTION: COMMUNICATIONS BETWEEN MODULES OF A COMPUTING APPARATUS

APPLICANT(S) FOR DO/EO/US: (1) Graeme John PROUDLER (2) David CHAN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This is an express request to promptly begin national examination procedures (35 U.S.C. 371(f)).
4. [X] The US has been elected by the expiration of 19 months from the priority date (PCT Article 31).
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [XX] is attached hereto (required only if not communicated by the International Bureau).
   b. [ ] has been communicated by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Ofice (RO/US).
6. [ ] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
7. [X] Amendments to the claims of the International Application under PCT Article 19(35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [ ] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [XX] have not been made and will not be made.
8. [X] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C371(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 16 below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [X] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information:

copy of Published Title Page of PCT International Application
Declaration/Power of Attorney executed by Graeme John PROUDLER
Declaration/Power of Attorney executed by David CHAN
copy of PCT Request
copy of PCT Demand
copy of International Preliminary Examination Report
Claim to Priority
copy of International Search Report (see Information Disclosure Statement)

533 Rec'd PCT/PTO 14 AUG 2001

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
not yet assigned 09/913453	PCT/GB00/00504	R-4276PCT 619003-1

17. [X] The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1000.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $860.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $710.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $690.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	30 - 20 =	10	X $18.00	$ 180.00	
Independent claims	2 - 3 =	0	X $80.00	$ 0	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)	0*		+ $270.00	$ 0	
TOTAL OF ABOVE CALCULATIONS =				$ 1040.00	
[ ] Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				$	
SUBTOTAL =				$ 1040	
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 1040.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$	
TOTAL FEES ENCLOSED =				$ 1040.00	
*Preliminary Amendment deleting multiple dependencies enclosed herewith.				**Amount to be refunded:**	$
				charged:	$

a. [X] A check in the amount of $ 1040.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 12-0415. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pendin g status.

SEND ALL CORRESPONDENCE TO:

LADAS & PARRY
5670 Wilshire Blvd., #2100
Los Angeles, California 90036-5679

Telephone No.: (323) 934-2300
Telefax No.: (323) 934-0202

August 14, 2001
DATE

SIGNATURE:

Richard P. Berg
NAME

28,145
REGISTRATION NUMBER

EL652176579US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Graeme John PROUDLER, et al.	Re: Preliminary Amendment
U.S. Appln. No.: not yet assigned	Group: not yet assigned
U.S. Filing Date: concurrently herewith	Examiner: not yet assigned
International Application No: PCT/GB00/00504	
International Filing Date: 15 February 2000	Our Ref.: B-4276PCT 619003-1
For: "COMMUNICATIONS BETWEEN MODULES OF A COMPUTING APPARATUS")	Date: August 14, 2001

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Attn: United States Designated/Elected Office (DO/EO/US)

Sir:

Prior to examination of the above-identified application, it is respectfully requested that the following amendments be made to the Claims:

IN THE CLAIMS

1. (Amended) A computing apparatus comprising:

a trusted hardware module;

a plurality of further hardware modules;

a shared communication infrastructure by which the hardware modules can communicate with each other; and

a first communication path, distinct from the shared communication infrastructure, by which a first one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

2. (Amended) An apparatus as claimed in claim 1, wherein the trusted hardware module and the first further hardware module each include a respective computing engine which partakes in the direct communication *via* the first communication path.

3. (Amended) An apparatus as claimed in claim 2, wherein:

the first further hardware module is operable to supply to the trusted hardware module a request for operation on data; and

in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first further hardware module *via* the first communication path and not *via* the shared communication infrastructure.

4. (Amended) An apparatus as claimed in claim 3, wherein the trusted hardware module includes means for storing policy information regarding such operations which can and/or cannot be permitted, and is operable to generate the response with reference to the policy information.

5. (Amended) An apparatus as claimed in claim 1, wherein the trusted hardware module is operable to generate an encryption and/or decryption key and to supply that key to the first further hardware module *via* the first communication path and not *via* the shared communication infrastructure.

6. (Amended) An apparatus as claimed in claim 5, wherein the first further hardware module is operable to use the key for encryption and/or decryption of data communicated *via* the shared communication infrastructure.

7. (Amended) An apparatus as claimed in claim 1, wherein the trusted hardware module is operable to generate a challenge and

to supply the challenge to the first further hardware module *via* the first communication path or *via* the shared communication infrastructure using encryption set up using the first communication path.

8. (Amended) An apparatus as claimed in claim 7, wherein:

in response to the challenge, the first further hardware module is operable to generate a response and to supply the response to the trusted hardware module *via* the first communication path or *via* the shared communication infrastructure using encryption set up using the first communication path; and

the trusted hardware module is operable to use the response in generating an integrity metric of the apparatus.

9. (Amended) An apparatus as claimed in claim 1, wherein:

the first further hardware module has a zone for private data and a zone for non-private data; and

the first further hardware module is operable to supply and/or receive data from/for the private data zone *via* the first communication path and not *via* the shared communication infrastructure.

10. (Amended) An apparatus as claimed in claim 9, wherein the first further hardware module is operable to supply and/or receive data from/for the non-private data zone *via* the shared communication infrastructure.

11. (Amended) An apparatus as claimed in claim 10, wherein the first further hardware module has an interface between the private and non-private data zones which is operable to inhibit the passing of data from the private data zone to the non-private data zone.

12. (Amended) An apparatus as claimed in claim 1, wherein the first further hardware module is a network interface module.

13. (Amended) An apparatus as claimed in claim 1, and including a second communication path, distinct from the shared communication infrastructure and the first communication path, by which a second one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

14. (Amended) An apparatus as claimed in claim 13, wherein:

the first further hardware module is operable to supply to the trusted hardware module a request for a transfer of data between the first and second further hardware modules; and

in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first or second further hardware module *via* the first or second communication path, as the case may be, and not *via* the shared communication infrastructure.

15. (Amended) An apparatus as claimed in claim 14, wherein the trusted hardware module includes means for storing policy information regarding such transfers which can and/or cannot be permitted, and is operable to generate the response with reference to the policy information.

16. (Amended) An apparatus as claimed in claim 14, wherein:

in response to an appropriate such transfer response, the first or second further hardware module is operable to supply the data to the trusted hardware module *via* the first or second communication path, as the case may be; and

in response to the receipt of such data, the trusted hardware module is operable to relay the data to the second or first further hardware module, as the case may be, *via* the second or first communication path, as the case may be.

17. (Amended) An apparatus as claimed in claim 13, wherein the second further hardware module is a main processor unit of the apparatus or a non-volatile data storage module.

18. (Amended) An apparatus as claimed in claim 13, and including at least a third communication path, distinct from the shared communication infrastructure and the other communication paths, by which at least a third one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

19. (Amended) An apparatus as claimed in claim 18, wherein the second further hardware module is a main processor unit of the apparatus and the third further hardware module is a non-volatile data storage module.

20. (Amended) An apparatus as claimed in claim 1, wherein the trusted hardware module is adapted to measure an integrity metric of the computing apparatus.

Please add the following new claims:

21. (New) A computing apparatus comprising:

a trusted hardware module resistant to unauthorized modification;

a plurality of further hardware modules;

a shared communication infrastructure by which the hardware

modules can communicate with each other; and

a first communication path distinct from the shared communication infrastructure by which a first one of the further hardware modules can communicate directly with the trusted hardware module but which is inaccessible to the other further hardware modules.

22. (New) An apparatus as claimed in claim 21, wherein the trusted hardware module and the first further hardware module each include a respective computing engine which partakes in the direct communication *via* the first communication path.

23. An apparatus as claimed in claim 22, wherein:
the first further hardware module is operable to supply to the trusted hardware module a request for operation on data; and
in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first further hardware module *via* the first communication path and not *via* the shared communication infrastructure.

24. (New) An apparatus as claimed in claim 23, wherein the trusted hardware module includes means for storing policy information regarding such operations which can and/or cannot be permitted, and is operable to generate the response with reference to the policy information.

25. (New) An apparatus as claimed in claim 21, wherein the trusted hardware module is operable to generate an encryption and/or decryption key and to supply that key to the first further hardware module *via* the first communication path and not *via* the shared communication infrastructure.

26. (New) An apparatus as claimed in claim 25, wherein the

first further hardware module is operable to use the key for encryption and/or decryption of data communicated *via* the shared communication infrastructure.

27. (New) An apparatus as claimed in claim 21, wherein the trusted hardware module is operable to generate a challenge and to supply the challenge to the first further hardware module *via* the first communication path or *via* the shared communication infrastructure using encryption set up using the first communication path.

28. (New) An apparatus as claimed in claim 27, wherein:
in response to the challenge, the first further hardware module is operable to generate a response and to supply the response to the trusted hardware module *via* the first communication path or *via* the shared communication infrastructure using encryption set up using the first communication path; and
the trusted hardware module is operable to use the response in generating an integrity metric of the apparatus.

29. (New) An apparatus as claimed in claim 21, wherein the first further hardware module is a network interface module.

30. (New) An apparatus as claimed in claim 21, wherein the trusted hardware module is adapted to measure an integrity metric of the computing apparatus.

REMARKS

This Preliminary Amendment removes the reference numerals from the claims and clarifies antecedents for some of the terms in the claims. These amendments do not affect the scope of the claims. New claims 21-30 have been added after International

Preliminary Examination.

This Preliminary Amendment also amends Claims 3, 5, 7, 9, 11-13, 16-18, and 20 so that these claims are no longer multiply dependent to reduce the official fees at the U.S. Patent and Trademark Office (USPTO). The Applicants may elect to amend Claims 3, 5, 7, 9, 11-13, 16-18, and 20 to make them again multiply dependent or to add additional claims to this application to provide coverage similar to, broader than, or narrower than the present claims at any time during the pendency of the above-identified U.S. application.

Respectfully submitted,

Richard P. Berg
Reg. No. 28,145
Attorney for Applicant
LADAS & PARRY
5670 Wilshire Boulevard #2100
Los Angeles, California 90036
(323) 934-2300

Enclosure: Appendix A (6 pages)

Appendix A

(VERSION WITH MARKINGS TO SHOW CHANGES MADE)

1. (Amended) A computing apparatus comprising:

a trusted hardware module [(120)];

a plurality of further hardware modules [(102,104,106)];

a shared communication infrastructure [(110)] by which the hardware modules can communicate with each other; and

a first communication path [(122a;122b;122c)], distinct from the shared communication infrastructure, by which a first one [(102;104;106)] of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

2. (Amended) An apparatus as claimed in claim 1, wherein the trusted hardware module and the first further hardware module each include a respective computing engine which partakes in the direct communication *via* the first communication path.

3. (Amended) An apparatus as claimed in claim [1 or] 2, wherein:

the first further hardware module [(102)] is operable to supply to the trusted hardware module a request [(156)] for operation on data; and

in response to such a request, the trusted hardware module is operable to generate a response [(158)] and to supply the response to the first further hardware module *via* the first communication path [(122a)] and not *via* the shared communication infrastructure.

Appendix A

(VERSION WITH MARKINGS TO SHOW CHANGES MADE)

4. (Amended) An apparatus as claimed in claim 3, wherein the trusted hardware module includes means [(132)] for storing policy information regarding such operations which can and/or cannot be permitted, and is operable to generate the response with reference to the policy information.

5. (Amended) An apparatus as claimed in [any preceding] claim 1, wherein the trusted hardware module is operable to generate an encryption and/or decryption key and to supply that key to the first further hardware module *via* the first communication path and not *via* the shared communication infrastructure.

6. (Amended) An apparatus as claimed in claim 5, wherein the first further hardware module is operable to use the key for encryption and/or decryption of data communicated *via* the shared communication infrastructure.

7. (Amended) An apparatus as claimed in [any preceding] claim 1, wherein the trusted hardware module is operable to generate a challenge [(142)] and to supply the challenge to the first further hardware module *via* the first communication path or *via* the shared communication infrastructure using encryption set up using the first communication path.

Appendix A

(VERSION WITH MARKINGS TO SHOW CHANGES MADE)

8. (Amended) An apparatus as claimed in claim 7, wherein:

in response to the challenge, the first further hardware module is operable to generate a response [(144a,144b,144c)] and to supply the response to the trusted hardware module *via* the first communication path or *via* the shared communication infrastructure using encryption set up using the first communication path; and

the trusted hardware module is operable to use the response in generating an integrity metric of the apparatus.

9. (Amended) An apparatus as claimed in [any preceding] claim 1, wherein:

the first further hardware module [(106)] has a zone [(114)] for private data and a zone [(116)] for non-private data; and

the first further hardware module is operable to supply and/or receive data from/for the private data zone *via* the first communication path [(122c)] and not *via* the shared communication infrastructure.

10. (Amended) An apparatus as claimed in claim 9, wherein the first further hardware module is operable to supply and/or receive data from/for the non-private data zone *via* the shared communication infrastructure.

11. (Amended) An apparatus as claimed in claim [9 or] 10, wherein the first further hardware module has an interface [(118)] between the private and non-private data zones which is operable to inhibit the passing of data from the private data zone to the non-private data zone.

Appendix A

(VERSION WITH MARKINGS TO SHOW CHANGES MADE)

12. (Amended) An apparatus as claimed in [any preceding] claim 1, wherein the first further hardware module is a network interface module [(106)].

13. (Amended) An apparatus as claimed in [any preceding] claim 1, and including a second communication path [(122a;122b)], distinct from the shared communication infrastructure and the first communication path [(122c)], by which a second one [(102;104)] of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

14. (Amended) An apparatus as claimed in claim 13, wherein:

the first further hardware module [(102)] is operable to supply to the trusted hardware module a request [(164)] for a transfer of data between the first and second further hardware modules; and

in response to such a request, the trusted hardware module is operable to generate a response [(164)] and to supply the response to the first or second further hardware module [(104)] *via* the first or second communication path [(122b)], as the case may be, and not *via* the shared communication infrastructure.

15. (Amended) An apparatus as claimed in claim 14, wherein the trusted hardware module includes means [(132)] for storing policy information regarding such transfers which can and/or cannot be permitted, and is operable to generate the response with reference to the policy information.

Appendix A

(VERSION WITH MARKINGS TO SHOW CHANGES MADE)

16. (Amended) An apparatus as claimed in claim 14 [or 15], wherein:

in response to an appropriate such transfer response, the first or second further hardware module is operable to supply the data to the trusted hardware module *via* the first or second communication path, as the case may be; and

in response to the receipt of such data, the trusted hardware module is operable to relay the data to the second or first further hardware module, as the case may be, *via* the second or first communication path, as the case may be.

17. (Amended) An apparatus as claimed in claim [any of claims] 13 [or 16], wherein the second further hardware module is a main processor unit [(102)] of the apparatus or a non-volatile data storage module [(104)].

18. (Amended) An apparatus as claimed in claim [any of claims] 13 [to 17], and including at least a third communication path [link (122b)], distinct from the shared communication infrastructure and the other communication paths [links (122a,122c)], by which at least a third one [(104)] of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other [(102,106)] of the further hardware modules.

19. (Amended) An apparatus as claimed in claim 18, wherein the second further hardware module is a main processor unit [(102)] of the apparatus and the third further hardware module is a non-volatile data storage module [(104)].

Appendix A

(VERSION WITH MARKINGS TO SHOW CHANGES MADE)

20. (Amended) An apparatus as claimed in [any preceding] claim 1, wherein the trusted hardware module [(120)] is adapted to measure an integrity metric of the computing apparatus.